

1       **Claims**

2  
3       1.    A financial transaction verification system comprising:

4  
5           a transaction processing client;

6  
7           a transaction processing server under the control of a financial services provider;

8  
9           a programmable telecommunications client under the control of a transaction  
10          initiator;

11  
12          the transaction processing client, the transaction processing server and the  
13          telecommunications client all being connected to or adapted for connection to a  
14          telecommunications network;

15  
16          the transaction processing client being adapted, when in use a transaction is  
17          initiated and processed through the transaction processing client, to record:

18  
19                 data pertaining to a transaction initiated, in use, by the transaction initiator;  
20                 and

21  
22                 data pertaining to a financial account of the transaction initiator with the  
23                 financial services provider;

24  
25          the transaction processing client being adapted to transmit the recorded data to the  
26          transaction processing server by way of the telecommunications network;

27  
28          the transaction processing server being adapted to make use of data pertaining to  
29          the transaction initiator and the telecommunications client previously stored with the  
30          financial services provider to formulate a transaction authorisation request to the  
31          telecommunications client;

32  
33          the transaction processing server being adapted to transmit the transaction  
34          authorisation request to the telecommunications client by way of the  
35          telecommunications network;

36  
37          the telecommunications client being programmed to require the entry of an  
38          authorisation code into the telecommunications client as a precondition for the

1 further processing of the transaction authorisation request; and

2  
3 the telecommunications client being programmed, further, to transmit a process  
4 outcome message to either or both the transaction processing server and the  
5 transaction processing client, which process outcome message:

6  
7 if the incorrect authorisation code is entered, is constituted by a transaction  
8 cancellation signal; and

9  
10 if the correct authorisation code is entered, is constituted by a transaction  
11 authorisation signal.

- 12  
13 2. A financial transaction verification system according to claim 1 in which the  
14 telecommunications client is a mobile communication device that is personal to the  
15 transaction initiator, in which system:

16  
17 the transaction initiator data previously stored with the financial services provider  
18 includes unique mobile communication device data, which is data that is unique to  
19 and stored in the mobile communication device;

20  
21 the transaction processing server is adapted to transmit the previously stored  
22 unique mobile communication device data to the mobile communication device  
23 together with the authorisation request;

24  
25 the mobile communication device is programmed, on receipt of the transmitted  
26 data, to compare the transmitted data to the equivalent unique mobile  
27 communication device data stored in the mobile communication device;

28  
29 the telecommunications client is programmed, further, to transmit a process  
30 outcome message to either or both the transaction processing server and the  
31 transaction processing client, which process outcome message may, alternatively,  
32 be constituted by a transaction cancellation signal or a transaction authorisation  
33 signal;

34  
35 the mobile communication device being programmed, further:

36  
37 if the comparison between the transmitted data and the equivalent data  
38 stored in the mobile communication device fails, to transmit a process

1 outcome message constituted by a transaction cancellation signal; and

2  
3 if the comparison is successful, to require the entry, into the mobile  
4 communication device, of the authorisation code previously provided as a  
5 precondition for the further processing of the transaction authorisation  
6 request; and

7  
8 if the incorrect authorisation code is entered, to transmit a process outcome  
9 message constituted by a transaction cancellation signal; and

10  
11 if the correct authorisation code is entered to transmit a process outcome  
12 message constituted by a transaction authorisation signal.

- 13  
14 3. A financial transaction verification system according to either of the preceding claims  
15 that is adapted:

16  
17 to cancel the transaction in the event of the receipt, by the telecommunications  
18 client, of a transaction cancellation signal; and

19  
20 to allow the transaction to proceed to finality in the event of the receipt, by the  
21 telecommunications client, of a transaction authorisation signal.

- 22  
23 4. A transaction processing client for use with a system according to any one of the  
24 preceding claims.

- 25  
26 5. A transaction processing server for use with a system according to any one of the  
27 preceding claims.

- 28  
29 6. A telecommunications server for use with a system according to any one of the  
30 preceding claims.

- 31  
32 7. A telecommunications client for use with a system according to any one of the  
33 preceding claims.

- 34  
35 8. A method of verifying a financial transaction comprising the steps of:

36  
37 initiating a transaction at a transaction processing client;

38

1 recording, by means of the transaction processing client, data pertaining to the  
2 transaction together with data pertaining to a financial account of the transaction  
3 initiator with a financial services provider;

4  
5 transmitting the data so recorded from the transaction processing client to a  
6 transaction processing server under control of the financial services provider, by  
7 way of a telecommunications network,

8  
9 supplying, to the transaction processing server, data previously stored with the  
10 financial services provider and pertaining to a telecommunications client which is  
11 under the control of the transaction initiator;

12  
13 transmitting an authorisation request pertaining to the initiated transaction to the  
14 telecommunications client;

15  
16 requiring, on receipt of such a transaction authorisation request, the entry into the  
17 telecommunications client, of an authorisation code as a precondition for the further  
18 processing of the transaction authorisation request;

19  
20 transmitting a process outcome message to either or both the transaction  
21 processing server and the transaction processing client, which process outcome  
22 message:

23  
24 if the incorrect authorisation code is entered, is constituted by a transaction  
25 cancellation signal; and

26  
27 if the correct authorisation code is entered, is constituted by a transaction  
28 authorisation signal.

- 29  
30 9. A method of verifying a financial transaction according to claim 8 in which the  
31 telecommunications client is a mobile communication device personal to the  
32 transaction initiator and data unique to and stored in the mobile communication  
33 device is stored by the financial services provider as part of the communications data  
34 pertaining to the transaction initiator, the method including the additional steps of:

35  
36 transmitting the unique mobile communication device data from the transaction  
37 processing server to the mobile communication device together with the  
38 authorisation request;

1  
2 in the mobile communication device, comparing, on receipt of the transmitted data  
3 and authorisation request, the transmitted unique mobile communication device  
4 data to the equivalent mobile communication device data stored in the mobile  
5 communication device; and

6  
7 if the comparison between the transmitted data and the equivalent data  
8 stored in the mobile communication device fails, transmitting a transaction  
9 cancellation signal to either or both the transaction processing server and  
10 the transaction processing client; and

11  
12 if the comparison is successful, requiring the entry of the authorisation code  
13 previously provided into the mobile communication device as a precondition  
14 for the further processing of the transaction authorisation request; and

15  
16 if the incorrect authorisation code is entered, transmitting a transaction  
17 cancellation signal to either or both the transaction processing server and  
18 the transaction processing client; and

19  
20 if the correct code is entered, transmitting a transaction authorisation signal  
21 to either or both the transaction processing server and the transaction  
22 processing client.

- 23  
24 10. A method of verifying a financial transaction according to either of claims 8 or 9  
25 which includes the additional steps of:

26  
27 canceling the transaction in the event of the receipt, by the telecommunications  
28 client, of a transaction cancellation signal; and

29  
30 allowing the transaction to proceed to finality in the event of the receipt, by the  
31 telecommunications client, of a transaction authorisation signal.

- 32  
33 11. A method of verifying a financial transaction according to claim 8 in which the  
34 transaction involves the use of a documentary negotiable instrument, the method  
35 comprising the steps of:

36  
37 initiating the transaction by a participating negotiable instrument issuer issuing the  
38 negotiable instrument manually;

1  
2 recording, by means of the transaction processing client, data pertaining to the  
3 transaction including predetermined data pertaining to the negotiable instrument;

4  
5 transmitting the data so recorded from the transaction processing client to the  
6 transaction processing server by way of the telecommunications network,

7  
8 transmitting, to either or both the financial services provider and the transaction  
9 processing server, a negotiable instrument issuer code unique to the negotiable  
10 instrument issuer, thereby to confirm, to the transaction processing server, the  
11 transmitted data pertaining to the transaction including the predetermined data  
12 pertaining to the negotiable instrument;

13  
14 recording, at the transaction processing server, the data so confirmed; and

15  
16 comparing, when in use the negotiable instrument is presented for payment, the  
17 data on the face of the documentary negotiable instrument with the data recorded  
18 in the transaction processing server in respect of that negotiable instrument.

19  
20 12. A method of operating a transaction processing server for use in a financial  
21 transaction verification method according to claim 11, the method comprising the  
22 steps of:

23  
24 receiving the entry of data pertaining to negotiable instruments from participating  
25 negotiable instrument issuers;

26  
27 receiving, from each participating negotiable instrument issuer and in respect of the  
28 data pertaining to each such negotiable instrument, a unique negotiable instrument  
29 issuer code;

30  
31 confirming the validity of each negotiable instrument issuer code so entered by  
32 comparing the negotiable instrument issuer code so entered with a negotiable  
33 instrument issuer code stored in the transaction processing server; and

34  
35 permitting a participating presentation point to gain access to the data stored in  
36 respect of a particular negotiable instrument when that negotiable instrument is  
37 presented for payment, thereby to allow comparison between the stored data and  
38 the data appearing on the face of the negotiable instrument.

1  
2 13. A method of verifying a financial transaction according to claim 8 in which the  
3 transaction involves the use of a communications enabled transaction terminal as the  
4 transaction processing client, the method including the steps of:

5  
6 with the use of the mobile communication device, formulating and encrypting, by  
7 means of a first encryption key and data unique to the mobile communication  
8 device, a transaction request to be transmitted to the transaction terminal and

9  
10 transmitting a transaction request directly to the transaction terminal with the use of  
11 the mobile communication device, using a method of communication for which the  
12 transaction terminal is enabled;

13  
14 transmitting the transaction request from the transaction terminal to the transaction  
15 processing server;

16  
17 at the transaction processing server:

18  
19 receiving the transaction request;

20  
21 identifying the mobile communication device using the data unique to the  
22 mobile communication device;

23  
24 retrieving the first encryption key, previously stored at the transaction  
25 processing server in respect of the mobile communication device;

26  
27 decrypting the encrypted transaction request using the first encryption key;

28  
29 processing the transaction request and generating a process outcome  
30 message pertaining to the result of processing of the transaction request;

31  
32 generating a second encryption key, storing the second encryption key in  
33 the transaction processing server;

34  
35 transmitting the second encryption key to the transaction terminal;

36  
37 encrypting the process outcome message using the second encryption key;  
38 and

transmitting the encrypted process outcome message to the mobile communication device;

at the mobile communication device, extracting and storing the second encryption key and transmitting the encrypted process outcome message to the transaction terminal; and

at the transaction terminal, decrypting the encrypted process outcome message and applying the decrypted process outcome message to actuate the transaction terminal.

14. A method of verifying a financial transaction according to claim 13 in which the second encryption key that is stored at the transaction processing server and in the mobile communication device is used, in a following transaction processing cycle as the first encryption key.
15. A method of verifying a financial transaction according to claim 14 in which the second encryption key is generated, every time the transaction processing cycle is repeated, with the use of code hopping techniques.
16. A method of verifying a financial transaction according to any one of claims 13 to 15 in which, in the process of encrypting the transaction request to be transmitted to the transaction processing server, the transaction request is encrypted with the use, in addition, of a code unique to the person requesting the transaction.